UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/613,004	07/10/2000	Richard D. Haney	PRC-001	9157

7590 02/13/2004

Falk & Fish
Post Office Box 2258
Morgan Hill, CA 95038

EXAMINER	
ALI, AHMEDUR R	

ART UNIT	PAPER NUMBER
2131	3

DATE MAILED: 02/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/613,004	Applicant(s) HANEY, RICHARD D.	
	Examiner Ahmedur Ali	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 July 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The application has been examined. Claims 1-5 are pending in this Office Action.

Information Disclosure Statement

2. The references cited in the IDS, PTO-1449, Paper No. 2, has been considered.

Drawings

3. New corrected drawings are required in this application because in Figures. 1-4 because of the following reasons: color drawings are not acceptable until petition is granted; pencil and non black ink not permitted; frasures, alterations, over writings, interlineations, fold, copy machine marks not accepted; lines, number, & letters not uniformly thick and well defined, clean, durable, and black (poor line quality). Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Claim Objections

4. Claims 3 and 4 are objected to because of the following informalities: In line 7 of claim 3, the word 'to' is inappropriately used twice. In line 14 of claim 3, the word "algorithem" is spelled incorrectly. In line 17 of claim 3, the word 'the' is inappropriately used twice. In line 29 of claim 3, the word 'seleted' is spelled incorrectly. In lines 9 and 10 of claim 4, the word 'travelling' is spelled incorrectly. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-5 are rejected under 35 U.S.C. 102(e) as being anticipated by Provino (U.S. Patent No. 6,557,037). With respect to claim 1, Provino teach a wide area network using the internet as a backbone (see abstract; Fig. 1), comprising:

a first dedicated line coupled to a first participating ISX/ISP provider of internet access (see col. 3, lines 37-62; col. 4, lines 61-67 to col. 5, lines 1-17);

a source router having a channel service unit having an output coupled to said first dedicated line (see col. 3, lines 59-67 to col. 4, lines 1-23);

a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being transmitted via the WAN interface to said source, router using any encryption method having a user definable key or keys, and for decrypting the payloads of any incoming upstream WAN packets arriving from said source router via said WAN interface using the same

encryption method and user definable key or keys that were used to encrypt the outgoing WAN packets (see col. 9, lines 46-67 to col. 10, lines 1-44);

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers (see col. 9, lines 32-67 to col. 10, lines 1-12);

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit and a second dedicated line to said router of said endpoint ISX/ISP provider (see col. 1, lines 38-45; col. 3, lines 59-67 to col. 4, lines 1-22);

a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said firewall functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source router via said private tunnel using the same encryption method used by said source firewall and the same user definable key or keys used by said source firewall circuit, and for decrypting any incoming packets from said source router arriving from said endpoint participating ISX/ISP provider using the same encryption protocol used by

said source firewall and the same user definable key or keys used by said source firewall circuit and transmitting the decrypted packets to said second device (see col. 9, lines 46-67 to col. 10, lines 1-44; col. 15, lines 21-57).

7. With respect to claim 2, Provino teach process for launching downstream AlterWAN packets addressed to an AlterWAN destination into a private tunnel coupling two AlterWAN destinations using the internet as a backbone and for launching non-AlterWAN packets into a normal internet traffic routing data path (see abstract; Fig. 1), comprising the steps:

receiving at a source firewall an incoming downstream wide area network packet from a workstation or other device at a first customer location said incoming downstream wide area network packet being either addressed to an AlterWAN destination or not an AlterWAN packet (see col. 8, lines 58-67 to col. 9, lines 1-31);

at said source firewall, using the destination address in said incoming downstream wide area network packet to determine if said packet is addressed to an AlterWAN destination coupled to said source firewall by a private tunnel using the internet as a backbone (hereafter referred to as an AlterWAN packet) or is addressed to some non-AlterWAN website or location on the internet (hereafter referred to as a non-AlterWAN packet) (see col. 10,lines 13-44);

if said packet is an AlterWAN packet, encrypting at said source firewall the payload portion thereof and forwarding the encrypted AlterWAN packet to a source router (see col. 10, lines 13-44);

if said packet is a non-AlterWAN packet, at said source firewall, forwarding said non-AlterWAN packet to said source router without encrypting the payload portion thereof (see col. 13,lines 26-53);

at said source router, converting both said AlterWAN packets and said non AlterWAN packets into signals suitable for transmission on a dedicated telephone line or other transmission medium coupling said source router to a specially selected first ISVISP provider and transmitting said signals to said specially selected ISX/ISP provider, said specially selected ISX/ISP provider being selected either because their routing tables are such that AlterWAN packets will naturally be routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider in said virtual private network or because the routing tables of the router of said first ISX/ISP provider have been altered to insure that AlterWAN packets get routed along high bandwidth, low hop-count data paths to the next ISX/ISP provider along said private tunnel (see col. 4, lines 50-67 to col. 5, lines 1-17).

8. With respect to claim 3, Provino teach an apparatus comprising:

a dedicated data path for coupling to a specially selected first participating ISX/ISP provider of internet access (see col. 3, lines 37-62; col. 4, lines 61-67 to col. 5, lines 1-17);

a firewall circuit having a first port for coupling directly or through a local area network to one or more devices for which communication over a wide area network using the internet as a backbone is desired, and having a second port, said

firewall functioning to use the destination addresses in the headers of each packet received from said one or more devices to distinguish between AlterWAN packets which are packets addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, and conventional packets which are packets not addressed to destination devices coupled to said firewall circuit via a private tunnel through the internet, said firewall circuit functioning to encrypt the payloads of outgoing AlterWAN packets using one or more predetermined keys and an encryption algorithm, and sending said encrypted AlterWAN packets to said source router via said second port, and functioning to forward any conventional packets to said source router, and functioning to decrypt any incoming AlterWAN packets arriving from said source router using the same encryption algorithms and one or more predetermined keys which were used to encrypt the packets at the location from which they were sent (see col. 9, lines 32-67 to col. 10, lines 1-44);

a source router having an input coupled to said second port of said firewall circuit either directly or by a local area network connection, and having a channel service unit having an output coupled to said dedicated data path, said channel service unit functioning to convert digital data packets received from said firewall circuit into signals suitable for transmission over whatever type of transmission medium is selected for said dedicated data path, and for converting signals received from said dedicated data path into data packets, said source router for transmitting both AlterWANI and non-AlterWAN packets over said dedicated data path to said specially selected first participating ISX/ISP provider where AlterWAN packets will be routed

via said private tunnel and specially selected ISX/ISP providers to their destination and non-AlterWAN packets will be routed along paths on the internet other than said private tunnel (see col. 9, lines 32-67 to col. 10, lines 1-44; col. 15, lines 21-57).

9. With respect to claim 4, Provino a method of designing and implementing a wide area network using the internet as a backbone (see abstract; Fig. 1), comprising the steps:

1) selecting source and destination sites that have devices that need to be connected by a wide area network (see Fig. 1);

2) examining the ISX/ISP internet service providers that exist between said source and destination sites and selecting two or more of such ISX/ISP providers through which data passing between said source and destination sites will be routed, said selection being based upon how many hops the routers at those sites will cause packets traveling between said source and destination sites to take and whether the average available bandwidth of the data paths along which the packets traveling between said source and destination sites will travel is substantially greater than the worst case bandwidth consumption of traffic between said source and destination sites (see col. 9, lines 32-67 to col. 10, lines 1-44);

3) coupling a source firewall to the devices at said source site and configuring said firewall to examine the destination addresses of packets received from said devices at said source site and encapsulate each packet addressed to any device at said destination site in an internet protocol packet, hereafter referred to as

an AlterWANI packet, said AlterWAN packet having as its destination address the address of an untrusted port of a destination firewall at said destination site and having the original IP packet as its payload, said source firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any packets received from said devices at said source site which are not addressed to any device at said destination site, and configuring said source firewall to recognize any incoming AlterWANI packets which have as their destination addresses the IP address of the untrusted side of said source firewall and to strip off the AlterWAN packet headers and decrypt the payload portion of each said AlterWAN packet to recover the original IP packet transmitted from said destination site using the same encryption algorithm and the same encryption key or keys used to encrypt the payload portions of said AlterWAN packets at said destination site and for outputting said recovered the original IP packet to said devices at said source site, said source firewall having an untrusted port (see col. 9, lines 32-67 to col. 10, lines 1-44; col. 15, lines 21-57);

4) coupling a source router to receive said encrypted and non-encrypted packets from said untrusted port of said source firewall and to convert them in a channel service unit to signals suitable for transmission over a first dedicated local loop connection (see Fig. 1);

5) contracting to establish said first dedicated local loop connection between the output of said source router at which said signals appear and a first participating

ISX/ISP provider in the group of ISVISP providers selected in step 2 (see Fig. 1);

6) providing a destination router at said destination site having a channel service unit which functions to receive from a second dedicated local loop connection downstream signals encoding both encrypted AlterWAN packet and conventional IP packets and converting said signals back into the original digital packet form and outputting the recovered downstream packets at a firewall port, and said destination router configured to receive upstream AlterWAN and conventional packets and convert them into signals suitable for transmission on said second dedicated data path coupling said destination router to an endpoint participating ISX/ISP provider in the group of ISX/ISP providers selected in step 2 and transmitting said signals on said second dedicated local loop connection (see col. 10, lines 34-67 to col. 11, lines 1-45);

7) contracting to provide a Second dedicated local loop connection connecting the input of said destination router to said endpoint participating ISX/ISP provider, said second dedicated local loop connection having sufficiently high bandwidth to handle the worst case traffic volume (see col. 13, lines 26-53);

8) providing a destination firewall having an untrusted port having an IP address coupled to said firewall port of said destination router to receive said recovered digital packets, and configuring said destination firewall to recognize as AlterWAN packets incoming recovered packets having as their destination address the IP address of said destination firewall untrusted input port and to strip off the AlterWAN packet header and decrypt the payload portion of said AlterWAN packet using the same encryption algorithm and encryption key or keys that were used to

encrypt the packet at said source firewall, and configuring said destination firewall to output the decrypted packets at an output coupled to devices at said destination site, and configuring said destination firewall to examine the destination addresses of upstream IP packets received from said devices at said destination site and encapsulate each upstream IP packet addressed to any device at said source site in another IP packet, hereafter referred to as an AlterWAN packet, said AlterWAN packet having as its destination address the IP address of an untrusted port of said source firewall at said source site and having the original IP packet as its payload, said destination firewall being configured to encrypt the payload portions of all said AlterWAN packets using a predetermined encryption algorithm and one or more encryption keys but not to encapsulate or encrypt the payload portions of any IP packets received from said devices at said destination site which are not addressed to any device at said source site (hereafter referred to as conventional packets), and said destination firewall configured to transmit said encrypted AlterWAN packets and said conventional packets to said destination router via said untrusted port (see col. 9, lines 32-67 to col. 10, lines 1-44; col. 13, lines 26-53; col. 15, lines 21-57).

10. With respect to claim 5, Provino a wide area network using the internet as a backbone (see abstract; Fig. 1), comprising:

a first dedicated line coupled to a first participating ISX/ISP provider of internet access (see col. 3, lines 37-62; col. 4,lines 61-67 to col. 5, lines 1-17);

a source router having a channel service unit having an output coupled to said

first dedicated line (see col. 3, lines 59-67 to col. 4, lines 1-23);

a source firewall circuit having a first port for coupling directly or through a local area network to a first device for which communication over said wide area network (hereafter WAN) is desired, and having a WAN interface coupled to said source router directly or through a local area network, said source firewall functioning to encrypt the payloads of downstream WAN packets being transmitted via the WAN interface to said source router using a first encryption method having a first set of user definable keys which may be only one key, and for decrypting the payloads of any incoming upstream WAN packets arriving from said first participating ISX/ISP using a second encryption method which is different than said first encryption method and a second set of user definable keys which are different than the first set of user definable keys were used to encrypt the downstream WAN packets (see col. 9, lines 46-67 to col. 10, lines 1-44);

one or more routers of other participating ISX/ISP providers of internet services including a router at an endpoint participating ISX/ISP provider, said routers functioning to implement a predetermined private tunnel data path coupling a router of said first ISX/ISP to a router of said endpoint participating ISX/ISP provider through said routers of said participating ISX/ISP providers (see col. 9, lines 32-67 to col. 10, lines 1-12);

a destination router including a channel service unit coupled to or part of said destination router, said destination router coupled through said channel service unit

and a second dedicated line to said router of said endpoint ISX/ISP provider (see col. 1, lines 38-45; col. 3, lines 59-67 to col. 4, lines 1-22);

a destination firewall circuit having a WAN interface coupled to said destination router directly or through a local area network and having a second port for coupling directly or through a local area network to a device for which communication across said wide area network is desired, said destination firewall functioning to encrypt the payloads of upstream WAN packets being transmitted through said WAN interface to said destination router for transmission to said source router via said private tunnel using the same encryption method and user definable key or keys used by said source firewall to decrypt upstream WAN packets, and for decrypting any incoming downstream WAN packets from said source router arriving from said destination router via the router of said endpoint participating ISX/ISP provider using the same encryption method and encryption key or keys used by said source firewall to encrypt downstream WAN packets and transmitting the decrypted packets to said second device (see col. 9, lines 46-67 to col. 10, lines 1-44; col. 19, lines 21-57).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Bots et al. (U.S. Patent No. 6,226,748) disclose an architecture for virtual private networks.

Gilbrech (U.S. Patent No. 6,173,399) discloses an apparatus for implementing virtual private networks.

Gore, Jr. et al. (U.S. Patent No. 5,862,029) disclose a secured gateway interface.

Schneider et al. (U.S. Patent No. 6,178,505) disclose a secure delivery of information in a network.

Wesinger, Jr. et al. (U.S. Patent No. 5,898,830) disclose a firewall providing enhanced network security and user transparency.

Engel et al. (U.S. Patent No. 6,519,636) disclose an efficient classification, manipulation, and control of network transmissions by associating network flows with rule based authentication.

Breslow et al. (U.S. Patent No. 6,493,342) disclose a method of data transmission in a data communication network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ahmedur Ali whose telephone number is 305-4667. The examiner can normally be reached on 8:30am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ara

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100